

Symantec™ AntiVirus for Handhelds - Corporate Edition Implementation Guide

Symantec™ AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager Implementation Guide

Symantec™ AntiVirus for Handhelds - Corporate Edition Implementation Guide and Symantec™ AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 1.0

PN: 10102125

Copyright Notice

Copyright © 2003 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and LiveUpdate are trademarks of Symantec Corporation. SESA, Symantec AntiVirus, Symantec Enterprise Security Architecture, and Symantec Security Response are trademarks of Symantec Corporation. Palm OS is a registered trademark, and Palm is a trademark of Palm, Inc. Microsoft, Outlook, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT

SYMANTEC ANTIVIRUS FOR HANDHELDS - CORP. ED.

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows.

YOU MAY:

- A. use each copy of the Software, indicated in the License Module, on up to two computers and a single handheld device as set forth in the documentation. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
- C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
- D. use the Software in accordance with any written agreement between You and Symantec; and
- E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

YOU MAY NOT:

- A. copy the printed documentation that accompanies the Software;
- B. use each licensed copy the Software on more than two computers, or for more than a single handheld device without purchasing additional licenses;
- C. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt

to discover the source code of the Software, or create derivative works from the Software;

D. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;

E. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

F. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

G. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor

H. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR

INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of the Software to any entity not authorized by or specifically prohibited by the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
 - Error messages/log files
 - Troubleshooting performed prior to contacting Symantec
 - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Technical support

Chapter 1 Introducing Symantec AntiVirus for Handhelds - Corporate Edition

About Symantec AntiVirus for Handhelds - Corporate Edition	10
Components of Symantec AntiVirus for Handhelds - Corporate Edition ..	10
How Symantec AntiVirus for Handhelds - Corporate Edition works	11
How handheld devices are protected	11
How virus protection and Symantec AntiVirus for Handhelds - Corporate Edition are updated	12
How histories are logged	13
How SESA management works	14
What you can do with Symantec AntiVirus for Handhelds - Corporate Edition	15
Where to get more information about Symantec AntiVirus for Handhelds - Corporate Edition	17

Chapter 2 Installing Symantec AntiVirus for Handhelds - Corporate Edition

About installing Symantec AntiVirus for Handhelds - Corporate Edition ..	20
System requirements	20
Licensing Symantec AntiVirus for Handhelds - Corporate Edition	21
Installing Symantec AntiVirus for Handhelds - Corporate Edition	23
Installing Symantec AntiVirus for Handhelds - Corporate Edition on the desktop	24
Installing Symantec AntiVirus for Handhelds - Corporate Edition using a remote administration tool	27
Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager	28
Reinstalling the handheld-resident component of Symantec AntiVirus for Handhelds - Corporate Edition	37
Testing and configuring the installation	37
Testing the installation	38
Uninstalling Symantec AntiVirus for Handhelds - Corporate Edition	38

Chapter 3	Scanning for and responding to viruses	
	About scanning for and responding to viruses	44
	Scan configuration options	44
	Using Auto-Protect to automatically scan files	45
	Using Auto-Protect on Palm OS handheld devices	45
	Using Auto-Protect on Pocket PC handheld devices	46
	Initiating an on-demand scan	46
	Configuring post-synchronization scans	47
	Scheduling repeating scans	47
	Configuring Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager	48
	Modifying general configuration settings in SESA	48
	Configuring post-synchronization scans in SESA	49
	Configuring scheduled scans in SESA	50
	Configuring and locking AntiVirus options in SESA	50
	Configuring LiveUpdate Wireless options in SESA	51
	Setting an administrator message in SESA	51
Chapter 4	Updating Symantec AntiVirus for Handhelds - Corporate Edition	
	About updating Symantec AntiVirus for Handhelds - Corporate Edition ..	54
	Using LiveUpdate to update Symantec AntiVirus for Handhelds - Corporate Edition	56
Chapter 5	Viewing and configuring histories, events, and alerts with Symantec AntiVirus for Handhelds - Corporate Edition	
	About histories, events, and alerts	60
	Working with histories on the handheld device	61
	Working with histories on the desktop	61
	Viewing and configuring events and alerts in SESA	66

Introducing Symantec AntiVirus for Handhelds - Corporate Edition

This chapter includes the following topics:

- [About Symantec AntiVirus for Handhelds - Corporate Edition](#)
- [Components of Symantec AntiVirus for Handhelds - Corporate Edition](#)
- [How Symantec AntiVirus for Handhelds - Corporate Edition works](#)
- [What you can do with Symantec AntiVirus for Handhelds - Corporate Edition](#)
- [Where to get more information about Symantec AntiVirus for Handhelds - Corporate Edition](#)

About Symantec AntiVirus for Handhelds - Corporate Edition

Symantec AntiVirus for Handhelds - Corporate Edition provides secure mobile computing through comprehensive, reliable protection against malicious code for Palm OS and Pocket PC handheld devices.

Components of Symantec AntiVirus for Handhelds - Corporate Edition

[Table 1-1](#) lists and describes the components of Symantec AntiVirus for Handhelds - Corporate Edition.

Table 1-1 Symantec AntiVirus for Handhelds - Corporate Edition components

Component	Description
Desktop component	Provides configuration and management of antivirus activities from the desktop.
Handheld device component	Provides real-time, on-demand, and scheduled virus scans on handheld devices. In addition, the handheld device component logs antivirus activities and uploads them to the desktop during synchronization.
LiveUpdate	Updates virus definitions files on the desktop. Depending on your configuration, LiveUpdate can obtain virus definitions update files from an internal LiveUpdate server or from the Symantec LiveUpdate server.
LiveUpdate Wireless	Allows users to update virus definitions files on handheld devices with wireless Internet connectivity. LiveUpdate Wireless obtains virus definitions files updates from the Symantec LiveUpdate server.
Symantec™ Enterprise Security Architecture (SESA) Agent	Available only if you have purchased a license for Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager. The SESA Agent is installed on the desktop and sends antivirus data to the SESA Manager. In addition, the SESA Agent provides communication functions between SESA and the desktop, allowing you to perform configuration management operations from the SESA Console.

Table 1-1 Symantec AntiVirus for Handhelds - Corporate Edition components

Component	Description
SESA Integration Package	Available only if you have purchased a license for Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager. The SESA Integration Package is installed on a computer running the SESA Manager. The Integration Package adds Symantec AntiVirus for Handhelds - Corporate Edition configuration, event management, and alerting functionality to the SESA Console.
Serial number certificate	Depending on how you purchased Symantec AntiVirus for Handhelds - Corporate Edition, the serial number certificate may be sent to you in the mail, delivered as an email attachment, or included in the box. You use the serial number to obtain a License File from the Symantec licensing Web site.

How Symantec AntiVirus for Handhelds - Corporate Edition works

Symantec AntiVirus for Handhelds - Corporate Edition consists of several components that work together to keep handheld devices protected from viruses.

How handheld devices are protected

Symantec AntiVirus for Handhelds - Corporate Edition uses virus definitions files to identify viruses. As files are accessed on the handheld device, Auto-Protect provides automatic, real-time virus scanning. In addition, users may also perform on-demand scans and scheduled scans. When Symantec AntiVirus for Handhelds - Corporate Edition scans a suspicious file, it blocks access to the file and presents users with a dialog box that allows them to delete the file or allow it.

Note: Auto-Protect handles virus scans on the different platforms in a slightly different manner. On Palm OS 3.5/4.x devices, Auto-Protect scans files before they are executed. On Palm OS 5.x devices, Auto-Protect scans files as they are executed. On Pocket PC devices, files are scanned whenever they are copied or moved.

Types of virus scans

Symantec AntiVirus for Handhelds - Corporate Edition supports four types of virus scanning, which are summarized in [Table 1-2](#).

Table 1-2 Types of virus scans

Scan type	Description
Auto-Protect	Real-time scanning continuously inspects files as they're accessed on the handheld device. Real-time protection is enabled by default. In a SESA environment, you can lock real-time protection settings if you want to enforce a virus policy. Users cannot change options that you lock.
Post-synchronization	Files are scanned after each synchronization.
On-demand	Manual or on-demand scans inspect selected files and folders on the handheld device.
Scheduled	Selected files and folders on the handheld device are scanned according to a predefined schedule.

What happens when Symantec AntiVirus for Handhelds - Corporate Edition finds a virus

When Symantec AntiVirus for Handhelds - Corporate Edition identifies a suspicious file, it does the following:

- Blocks access to the file
 - Displays a dialog box on the handheld device that provides information about the potentially infected file, and provides the option of deleting or allowing the suspicious file
 - Logs the found virus as an event
- See “[About scanning for and responding to viruses](#)” on page 44.

How virus protection and Symantec AntiVirus for Handhelds - Corporate Edition are updated

Symantec Security Response provides Symantec customers with regular virus definitions files updates to keep their virus protection current. In addition, Symantec may provide software updates that fix issues with Symantec AntiVirus for Handhelds - Corporate Edition.

Symantec AntiVirus for Handhelds - Corporate Edition offers the following two methods for updating virus definitions files:

- **LiveUpdate:** LiveUpdate on the desktop can pull virus definitions files updates directly from the Symantec LiveUpdate server or an internal LiveUpdate server and automatically update a handheld device the next time that it is synchronized. For handheld devices that infrequently or never synchronize with a desktop, Symantec AntiVirus for Handhelds - Corporate Edition can use LiveUpdate Wireless and a wireless Internet connection to connect to the Symantec LiveUpdate server and obtain virus definitions files updates.
- **Symantec AntiVirus Corporate Edition integration:** Symantec AntiVirus for Handhelds - Corporate Edition seamlessly integrates with Symantec AntiVirus Corporate Edition virus definitions files update methods. You can leverage your current update methods to update antivirus protection for both desktops and handheld devices.

See [“About updating Symantec AntiVirus for Handhelds - Corporate Edition”](#) on page 54.

How histories are logged

Symantec AntiVirus for Handhelds - Corporate Edition records the following information about the actions that are performed on the handheld device as well as the desktop:

- Viruses found
- Virus scans
- Configuration changes
- Synchronizations between handheld devices and the desktop
- Virus definitions files and software updates

The handheld device maintains a local cache of history data that can be viewed directly on the handheld device. When the handheld device is synchronized with its desktop, the event log automatically uploads to the desktop, and can be viewed and managed on the desktop.

In a SESA environment, the SESA Agent forwards log data to the SESA Manager. Events are viewable in the SESA Console, and if configured, the events can trigger alerts.

See [“About histories, events, and alerts”](#) on page 60.

How SESA management works

Product installation for the Event and Configuration Manager licensed product installs the SESA Agent on the desktop. The SESA Agent forwards the desktop's event data to the SESA Manager, where it may be viewed in the SESA Console. The installation also installs a SESA Integration Package that provides product configuration in the SESA Console.

See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager”](#) on page 28.

See [“Configuring scheduled scans in SESA”](#) on page 50.

See [“Configuring and locking AntiVirus options in SESA”](#) on page 50.

See [“Viewing and configuring events and alerts in SESA”](#) on page 66.

What you can do with Symantec AntiVirus for Handhelds - Corporate Edition

Table 1-3 summarizes what you can do with Symantec AntiVirus for Handhelds - Corporate Edition.

Table 1-3 Symantec AntiVirus for Handhelds - Corporate Edition features

Feature	Description
Protect handheld devices with real-time and on-demand scanning for viruses.	<p>Auto-Protect continuously scans for malicious code on the handheld device. With Auto-Protect, suspicious files cannot be opened without the user's permission. When Auto-Protect identifies a suspicious file, users have the option of deleting, not opening, or opening the file. In addition, users can perform on-demand scans, automatic scans when new files are downloaded, and scheduled scans.</p> <p>See "Types of virus scans" on page 12.</p>
Automatically update virus protection.	<p>Symantec AntiVirus for Handhelds - Corporate Edition employs virus definitions files that contain a list and details of known Palm OS or Pocket PC viruses. If configured, the desktop automatically receives virus definitions update files and updates the protection on the handheld devices with which it synchronizes. For handheld devices with Internet connectivity, LiveUpdate Wireless can update the device with the latest virus definitions and product updates over the Internet. For environments that use Symantec AntiVirus Corporate Edition, virus definitions can be transparently rolled out to all desktops that use Symantec AntiVirus for Handhelds - Corporate Edition.</p> <p>See "About updating Symantec AntiVirus for Handhelds - Corporate Edition" on page 54.</p>

Table 1-3 Symantec AntiVirus for Handhelds - Corporate Edition features

Feature	Description
Monitor antivirus activity.	<p>The Activity Log provides key information about protection and configuration. The Activity Log provides access to antivirus activities including partial scans, full scans, found viruses, deleted infected files, and failures to delete infected files. During synchronization, comprehensive data reporting on virus activity, scan history, and other event history is transferred to the desktop, and is viewable on the desktop through the History screen.</p> <p>See “About histories, events, and alerts” on page 60.</p> <p>See “Viewing and configuring events and alerts in SESA” on page 66.</p>
Protect multiple handheld devices from the same desktop.	<p>Users who use more than one handheld device can protect and monitor them all from the same desktop.</p> <p>See “Licensing Symantec AntiVirus for Handhelds - Corporate Edition” on page 21.</p>
Protect both Palm OS and Pocket PC handheld devices.	<p>Symantec AntiVirus for Handhelds - Corporate Edition supports handheld devices based on the Palm OS and Microsoft Pocket PC platforms.</p> <p>See “System requirements” on page 20.</p>
Centrally manage and configure Symantec AntiVirus for Handhelds - Corporate Edition.	<p>If you have purchased a license that includes event and configuration management, you can use the Symantec Enterprise Security Architecture (SESA) Console to centrally control configuration management and receive and manage events and alerts.</p> <p>See “Viewing and configuring events and alerts in SESA” on page 66.</p> <p>See “Configuring Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager” on page 48.</p>

Table 1-3 Symantec AntiVirus for Handhelds - Corporate Edition features

Feature	Description
Perform a silent installation.	<p>If you use a remote administration tool, you may install Symantec AntiVirus for Handhelds - Corporate Edition on remote desktops without requiring user interaction.</p> <p>See “Installing Symantec AntiVirus for Handhelds - Corporate Edition using a remote administration tool” on page 27.</p>

Where to get more information about Symantec AntiVirus for Handhelds - Corporate Edition

You can find additional information in the following sources:

- Readme.txt for late-breaking news
 Readme.txt is located in the SAH folder on the Symantec AntiVirus for Handhelds - Corporate Edition CD.
- www.symantec.com
- *Symantec Enterprise Security Architecture Administrator's Guide*

Installing Symantec AntiVirus for Handhelds - Corporate Edition

This chapter includes the following topics:

- [About installing Symantec AntiVirus for Handhelds - Corporate Edition](#)
- [System requirements](#)
- [Licensing Symantec AntiVirus for Handhelds - Corporate Edition](#)
- [Installing Symantec AntiVirus for Handhelds - Corporate Edition](#)
- [Reinstalling the handheld-resident component of Symantec AntiVirus for Handhelds - Corporate Edition](#)
- [Testing and configuring the installation](#)
- [Uninstalling Symantec AntiVirus for Handhelds - Corporate Edition](#)

About installing Symantec AntiVirus for Handhelds - Corporate Edition

A Symantec AntiVirus for Handhelds - Corporate Edition installation consists of the following:

- Reviewing the system requirements for installing Symantec AntiVirus for Handhelds - Corporate Edition
- Licensing Symantec AntiVirus for Handhelds - Corporate Edition
- Installing Symantec AntiVirus for Handhelds - Corporate Edition on the desktop and the handheld device
- For SESA environments, installing the SESA Agent on the desktop and a SESA Integration Package on the SESA server
- Testing and configuring the installation

System requirements

Following are the software requirements for Symantec AntiVirus for Handhelds - Corporate Edition:

- Windows 98/Windows 98 Second Edition (no SESA support)
- Windows Millennium Edition (Windows Me) (no SESA support)
- Windows NT 4.0 SP 6a (Workstation and Server)
- Windows 2000 Professional, SP 2 or later
- Windows 2000 Server/Advanced Server, SP 2 or later
- Windows XP (Home and Professional)
- Windows Server 2003 (no SESA support)
- Java Runtime Environment 1.4.1_02 or later
- Internet Explorer 5.5 or later
- Palm OS 3.5 or later
- Palm OS: HotSync Manager version 3.0.4 or later (available with Palm OS Desktop 3.1 or later); for Windows XP, Palm OS Desktop 4.1 or later

- Pocket PC 2002
- Pocket PC: Microsoft ActiveSync 3.5 or later

Note: Before you install Symantec AntiVirus for Handhelds - Corporate Edition, the consumer version of Symantec AntiVirus for Handhelds must be uninstalled from both the handheld device and the desktop.

[Table 2-1](#) lists hardware requirements for Symantec AntiVirus for Handhelds - Corporate Edition.

Table 2-1 Hardware requirements

Operating system/component	Requirements
Windows 98/Windows 98 Second Edition/ Windows Millennium Edition (Windows Me)	<ul style="list-style-type: none"> ■ Pentium 100 MHz (Pentium 150 MHz required for Windows Me) ■ 58 MB of RAM (without SESA); 68 MB RAM (with SESA) ■ 25 MB of hard disk space (without SESA); 45 MB of hard disk space (with SESA)
Windows NT 4.0 SP 6a (all versions)	<ul style="list-style-type: none"> ■ Pentium 100 MHz ■ 58 MB of RAM (without SESA); 68 MB RAM (with SESA) ■ 25 MB of hard disk space (without SESA); 45 MB of hard disk space (with SESA)
Windows 2000/Windows XP (all versions)	<ul style="list-style-type: none"> ■ Pentium 233 MHz ■ 58 MB of RAM (without SESA); 68 MB RAM (with SESA) ■ 25 MB of hard disk space (without SESA); 45 MB of hard disk space (with SESA)
Installation footprint	<ul style="list-style-type: none"> ■ Palm OS: 230 KB ■ Pocket PC: 445 KB
LiveUpdate Wireless	Wireless Internet hardware support using the regular TCP/IP stack. LiveUpdate using the modem of a Palm OS VII or m70x is unsupported.

Licensing Symantec AntiVirus for Handhelds - Corporate Edition

Licensing Symantec AntiVirus for Handhelds - Corporate Edition requires a serial number, which is provided on a serial number certificate. Depending on how you purchased Symantec AntiVirus for Handhelds - Corporate Edition, the

serial number may be sent to you in the mail, delivered as an email attachment, or included in the box. You will use the serial number to obtain a License File from the Symantec licensing Web site. As part of the licensing process, Symantec sends you a single License File as an email attachment. The license is good for one year, and is valid for the number of licenses purchased.

During installation, the desktop synchronizes with and licenses the handheld device. A License File must be distributed to the desktop to which the handheld device synchronizes. Once licensed, the desktop updates the virus definitions update files on a licensed handheld device for the duration of the license period. When the license expires, you are no longer entitled to receive virus definitions updates for Symantec AntiVirus for Handhelds - Corporate Edition. You should either renew the license or uninstall Symantec AntiVirus for Handhelds - Corporate Edition at that time.

Licensing for desktops that synchronize with multiple handheld devices and handheld devices that synchronize with multiple desktops works as follows:

- For environments in which multiple users share the same desktop, the same License File permits updates for any handheld device that shares the same license.
- A desktop may host multiple licenses and update any handheld device that has a license that matches a license on the desktop.
- A handheld device may only host a single license and may only be updated by desktops that have a matching license.

License Symantec AntiVirus for Handhelds - Corporate Edition

The licensing process consists of obtaining a License File from Symantec and distributing the file to the desktop. Depending on how you purchased Symantec AntiVirus for Handhelds - Corporate Edition, the serial number certificate may be sent to you in the mail, delivered as an email attachment, or included in the box.

To obtain a License File

- 1 Locate the serial number certificate for Symantec AntiVirus for Handhelds - Corporate Edition.
- 2 Point your Web browser to <https://licensing.symantec.com>
- 3 Follow the on-screen instructions.

Symantec sends you the License File as an email attachment. Save the attachment to a location that is easy to remember.

To distribute a license

- ◆ Do one of the following:
 - On the target installation desktop, copy the License File to C:\Program Files\Common Files\Symantec Shared\Licenses.
 - Use a remote administration tool such as Microsoft Systems Management Server (SMS), HP OpenView, CA Unicenter, Novell ZENworks, or IBM Tivoli to distribute the License File to C:\Program Files\Common Files\Symantec Shared\Licenses on remote desktops.
 - Use Symantec License Installer Creator to create a small application that contains the License File and provide the application to users. When users run the application, they will install the License File in the correct location. The Symantec License Installer Creator application, slfdist.exe, is located in the Support\tools folder on the CD. An Adobe Acrobat file that documents this tool, pkg_lic.pdf, is located in the Manual folder on the CD.

Installing Symantec AntiVirus for Handhelds - Corporate Edition

The installation procedure varies depending on how and what you are installing. You can install Symantec AntiVirus for Handhelds - Corporate Edition using the following installation options:

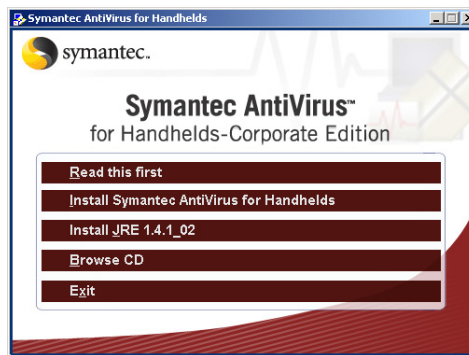
- On the desktop: Install Symantec AntiVirus for Handhelds - Corporate Edition directly on the desktop.
See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition on the desktop”](#) on page 24.
- Using a remote administration tool: Roll out Symantec AntiVirus for Handhelds - Corporate Edition silently using a remote administration tool.
See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition using a remote administration tool”](#) on page 27.
- With Event and Configuration Manager: To install a SESA-enabled product, you need to install the SESA Agent on the desktop and a SESA Integration Package on the SESA server.
See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager”](#) on page 28.

Installing Symantec AntiVirus for Handhelds - Corporate Edition on the desktop

If the handheld device is not available during installation, the software automatically installs when the handheld device synchronizes with the desktop.

To install Symantec AntiVirus for Handhelds - Corporate Edition on the desktop

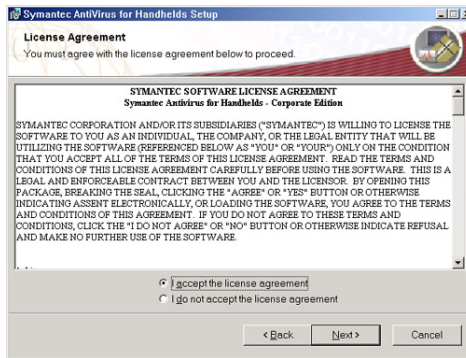
- 1 Insert the Symantec AntiVirus for Handhelds - Corporate Edition CD into your CD-ROM drive.



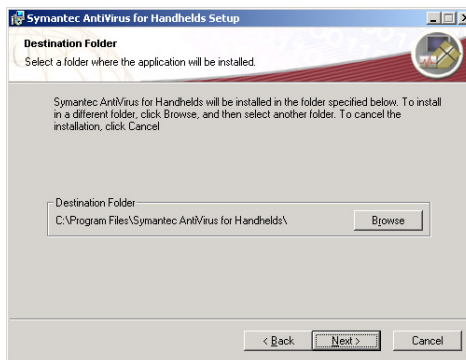
- 2 In the Symantec AntiVirus for Handhelds window, click **Install Symantec AntiVirus for Handhelds**.



- 3 In the Symantec AntiVirus for Handhelds Setup window, click **Next**.

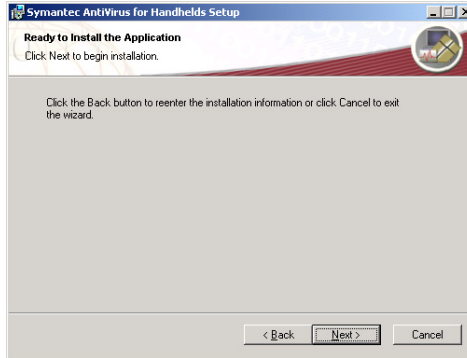


- 4 In the License Agreement window, click **I accept the license agreement**, then click **Next**.



- 5 In the Destination Folder window, select one of the following:

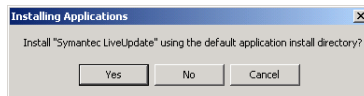
- Next: Accepts the default installation directory
- Browse: Selects a different installation directory



6 In the Ready to Install the Application window, select one of the following:

- Next: Starts the installation
- Back: Lets you modify installation settings

The desktop-resident components are installed first, and then the handheld device components. If the handheld device is available during installation, the installer asks if you want to install LiveUpdate and Symantec AntiVirus for Handhelds - Corporate Edition on the handheld device in the default directory. For desktops that synchronize with more than one Pocket PC, the installer prompts for the installation directories for each Pocket PC. For Palm OS handheld devices, the installer prompts only once.



7 Select one of the following:

- Yes: Installs LiveUpdate to the default directory
- No: Selects an alternate installation directory
- Cancel: Does not install LiveUpdate on the handheld device

If the handheld device is not available during installation, Symantec AntiVirus for Handhelds - Corporate Edition prompts you to select an installation directory when the handheld device is available.

- 8 If you chose to use LiveUpdate, in the LiveUpdate window, click **Next**, then follow the on-screen instructions to update Symantec AntiVirus for Handhelds - Corporate Edition.
- 9 Click **Finish**.
 See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager”](#) on page 28.
 See [“Testing the installation”](#) on page 38.

Installing Symantec AntiVirus for Handhelds - Corporate Edition using a remote administration tool

Symantec AntiVirus for Handhelds - Corporate Edition leverages Microsoft Installer technology, allowing you to use a remote administration tool such as Microsoft SMS, HP OpenView, CA Unicenter, Novell ZENworks, or IBM Tivoli to roll out Symantec AntiVirus for Handhelds - Corporate Edition on remote desktops.

Following are the supported Microsoft Installer installation options:

No user interface	The installation is completely silent.
Basic user interface	The user will see a progress indicator and error dialog boxes.
Reduced user interface	The installation Wizard is suppressed. Use this option if you plan on authoring your own installation.

Installing Symantec AntiVirus for Handhelds - Corporate Edition using a remote installation tool entails running the installation package on a remote desktop; installation switches determines how the installation appears on the remote desktop.

To install Symantec AntiVirus for Handhelds - Corporate Edition using a remote administration tool

- 1 Insert the Symantec AntiVirus for Handhelds - Corporate Edition CD into your CD ROM drive.
- 2 Copy SAH/sah.msi to a location accessible to your remote administration tool.
- 3 Configure your remote administration tool to roll out sah.msi using one of the following arguments:
 - No user interface: `msiexec /i sah.msi /qn`

- Basic user interface: `msiexec /i sah.msi /qb`
- Reduced user interface: `msiexec /i sah.msi /qr`

Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager

Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager consists of installing the desktop and handheld device components, the SESA Agent, and the SESA Integration Package. SESA supports a single configuration profile for each desktop. If you are installing the SESA-enabled product on a desktop that synchronizes with more than one handheld device, all handheld devices that synchronize with that desktop share the same configuration. If, however, you unlock a configuration setting from the SESA Console, each profile can have a unique configuration for that setting.

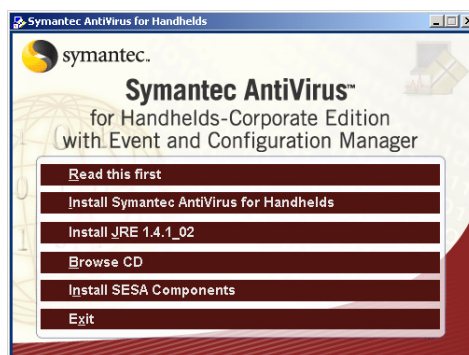
See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition on the desktop”](#) on page 24.

Install Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager

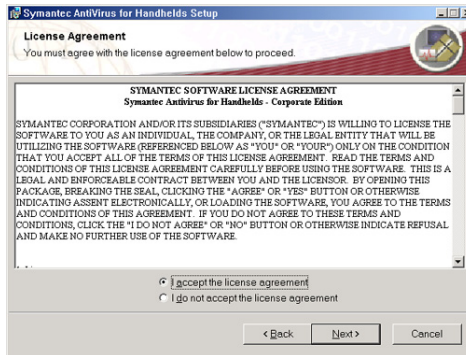
In a SESA-enabled installation, all of the components that are required to centrally manage Symantec AntiVirus for Handhelds - Corporate Edition from the SESA Console are installed. If you are installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager on a remote desktop, you must also install the SESA Agent on the remote desktop.

To install the handheld device and desktop components

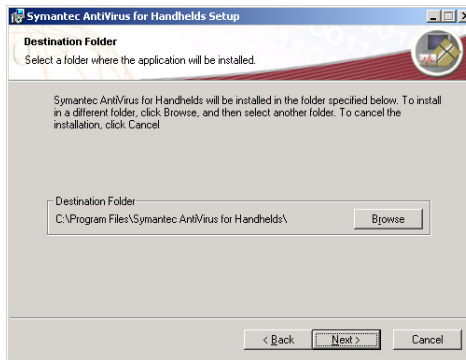
- 1 Insert the Symantec AntiVirus for Handhelds - Corporate Edition CD into your CD-ROM drive.



- 2 In the Symantec AntiVirus for Handhelds window, click **Install Symantec AntiVirus for Handhelds**.
- 3 In the Symantec AntiVirus for Handhelds Setup window, click **Next**.

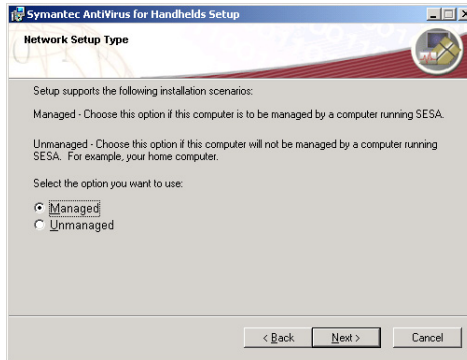


- 4 In the License Agreement window, click **I accept the license agreement**, then click **Next**.



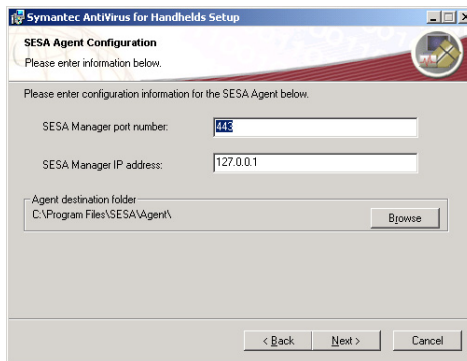
5 In the Destination Folder window, select one of the following:

- Next: Accepts the default installation directory
- Browse: Selects a different installation directory

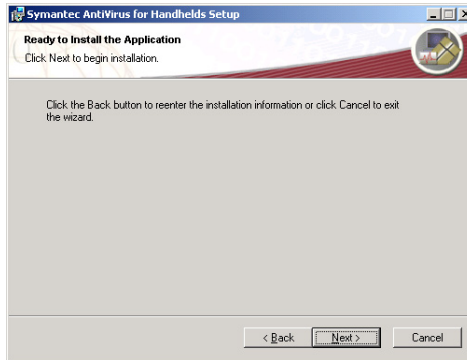


6 In the Network Setup Type window, select one of the following, then click **Next**:

- Managed: Installs the SESA management components
- Unmanaged: Does not install the SESA management components



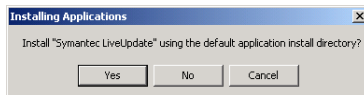
- 7 In step 7, if you clicked Managed, in the SESA Agent Configuration window, type the SESA Manager port number and SESA Manager IP address then click **Next**.



- 8 In the Ready to Install the Application window, select one of the following:

- **Next:** Starts the installation
- **Back:** Lets you modify installation settings

The installer first installs the desktop component, then the handheld device component. If the handheld device can synchronize with the desktop during installation, the installer asks if you want to install LiveUpdate and Symantec AntiVirus for Handhelds - Corporate Edition on the handheld device in the default directory.



- 9 Select one of the following:

- **Yes:** Installs LiveUpdate to the default directory
- **No:** Selects an alternate installation directory
- **Cancel:** Does not install LiveUpdate on the handheld device

If the handheld device is not available during installation, Symantec AntiVirus for Handhelds - Corporate Edition prompts you to select installation directory options when the handheld device is available.

10 If you chose to use LiveUpdate, in the LiveUpdate window, click **Next**, then follow the on-screen instructions to update Symantec AntiVirus for Handhelds - Corporate Edition.

11 Click **Finish**.

See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition on the desktop”](#) on page 24.

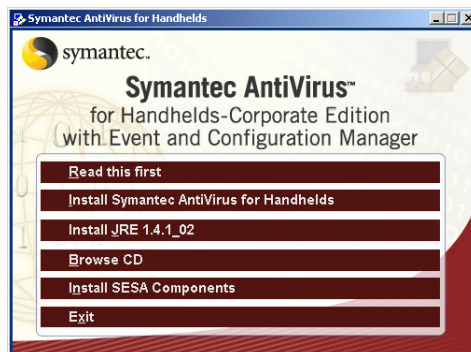
See [“Testing and configuring the installation”](#) on page 37.

To install the SESA Agent using a remote administration tool

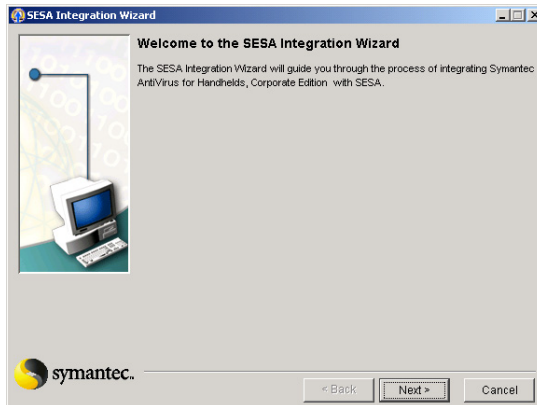
- 1 Insert the Symantec AntiVirus for Handhelds - Corporate Edition CD into your CD ROM drive.
- 2 Copy the SAH folder to a location accessible to your remote administration tool.
- 3 Edit the agent.settings file located in the SAH folder to conform to your network environment. The agent.settings file is self-documenting, and provides the settings that you would provide during an interactive installation.
- 4 Configure your remote administration tool to roll out sah.msi using one of the following arguments:
 - No user interface: `msiexec /i sah.msi /qn`
 - Basic user interface: `msiexec /i sah.msi /qb`
 - Reduced user interface: `msiexec /i sah.msi /qr`

To install the SESA Integration Package

- 1 Insert the Symantec AntiVirus for Handhelds - Corporate Edition CD into the CD-ROM drive of the computer on which the SESA Manager is installed.



- 2 In the Symantec AntiVirus for Handhelds window, click **Install SESA Components**.



- 3 In the Welcome to the SESA Integration Wizard window, click **Next**.



- 4 In the SESA Integration Requirements window, review the requirements, then click **Next**.

SESA Integration Wizard

XXXX...

SESA Domain Administrator Information

Enter the following information regarding the SESA Directory:
Username, Password, Host or IP Address, and Port number.

administrator SESA Domain Administrator Name

***** SESA Domain Administrator Password

255.255.255.255 Host Name or IP Address of SESA Directory

636 Secure Directory Port

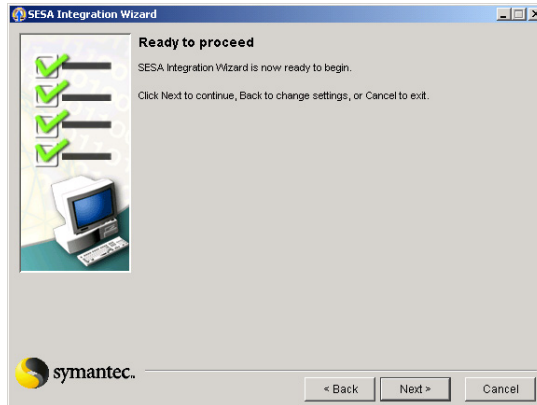
Status
SESA Directory Connection Pending

symantec.

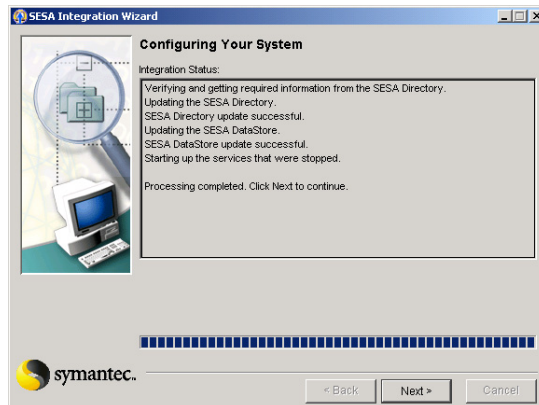
< Back Next > Cancel

- 5 In the SESA Domain Administrator Information window, type the following, then click **Next**:
- The SESA Domain Administrator name
 - The SESA Domain Administrator password

- The host name or IP address of the SESA Directory
- The Secure Directory port



6 In the Ready to proceed window, click **Next**.



- 7 When the installation is complete, the Configuring Your System window displays the message “Processing completed. Click Next to continue.” Click **Next** to continue.



- 8 In the SESA Integration Successful window, click **Finish**.
- 9 Verify SESA integration by logging onto the SESA Console.



The SESA Console should contain a configuration for Symantec AntiVirus for Handhelds, Corporate Edition.

See [“Testing and configuring the installation”](#) on page 37.

See [“Uninstalling Symantec AntiVirus for Handhelds - Corporate Edition”](#) on page 38.

Reinstalling the handheld-resident component of Symantec AntiVirus for Handhelds - Corporate Edition

If the handheld-resident component of Symantec AntiVirus for Handhelds - Corporate Edition is damaged or deleted (for example, if the handheld device's operating system was reinstalled), you can reinstall the software on the handheld device from the desktop-resident component.

For desktops that support multiple devices, the reinstall feature behaves slightly differently, depending on the type of handheld device. For Palm OS handheld devices, the reinstall feature reinstalls the software to all profiles. For Pocket PC handheld devices, the reinstall feature reinstalls the software on the Pocket PC currently in the cradle. If there isn't any Pocket PC in the cradle, the software is installed on the next Pocket PC that synchronizes with the desktop.

Note: Do not use ActiveSync to reinstall Symantec AntiVirus for Handhelds - Corporate Edition on handheld devices: Only use the following method.

To reinstall the handheld-resident component of Symantec AntiVirus for Handhelds - Corporate Edition

- ◆ On the desktop, click **File > Re-install Software on Devices**.
If there is a handheld device in the cradle, the software will be reinstalled immediately. If there is no handheld device in the cradle, the software will be reinstalled the next time that the handheld device is synchronized.

Testing and configuring the installation

After installation, you can do the following:

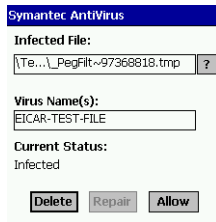
- Test the installation.
See [“Testing the installation”](#) on page 38.
- Configure Symantec AntiVirus for Handhelds - Corporate Edition to scan for viruses.
See [“Scanning for and responding to viruses”](#) on page 43.
- For SESA-enabled installations, configure the handheld device in SESA.
See [“Configuring Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager”](#) on page 48.

Testing the installation

For Pocket PC handheld devices only, you can verify that Symantec AntiVirus for Handhelds - Corporate Edition is active by downloading the standard European Institute for Computer Anti-Virus Research (EICAR) test file, and copying it to the handheld device. You can download the test file from www.eicar.org.

Note: You may need to temporarily disable antivirus scanning on the desktop in order to access the EICAR test file. Make sure to reenale antivirus scanning on the desktop when you are finished.

A successful installation of Symantec AntiVirus for Handhelds - Corporate Edition displays a dialog box when the EICAR test file is copied to the handheld device.



Uninstalling Symantec AntiVirus for Handhelds - Corporate Edition

Uninstalling Symantec AntiVirus for Handhelds - Corporate Edition requires uninstalling the desktop component, the handheld device component, and the SESA Integration Package.

Uninstall Symantec AntiVirus for Handhelds - Corporate Edition

Begin the uninstallation by first uninstalling the handheld device component and then the desktop component. Additional steps are required for uninstalling the SESA Integration Package.

Note: Uninstalling Symantec AntiVirus for Handhelds - Corporate Edition from the SESA Manager deletes the corresponding Symantec AntiVirus for Handhelds - Corporate Edition entries and data in the SESA Directory and SESA DataStore. Only uninstall if you intend to entirely remove Symantec AntiVirus for Handhelds - Corporate Edition from SESA.

To uninstall the handheld device component

- ◆ Follow the instructions for your handheld device for removing programs and remove both Symantec AntiVirus for Handhelds - Corporate Edition and LiveUpdate from the handheld device.

To uninstall the desktop component

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel window, double-click **Add/Remove Programs**.
- 3 In the Add/Remove Programs window, click **Symantec AntiVirus for Handhelds**.
- 4 Click **Remove**, then follow the on-screen instructions.

To uninstall the SESA Integration Package

- 1 On a computer on which the SESA Manager is installed, insert the Symantec AntiVirus for Handhelds - Corporate Edition CD into the CD-ROM drive.
- 2 At the command prompt, change directories on the CD to SAH\SESA.

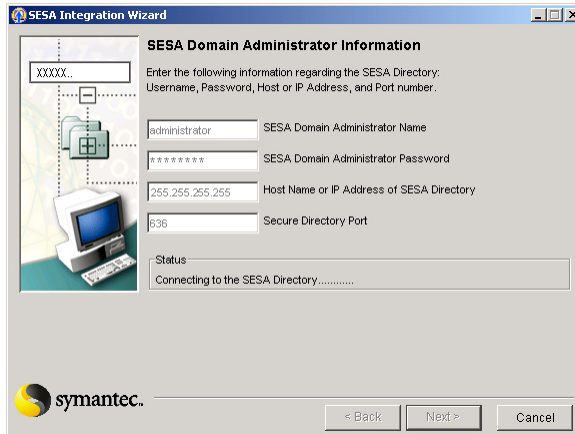
- 3 Type the following command to launch the SESA Integration Wizard:
java -jar setup.jar -uninstall



- 4 In the Welcome to the SESA Integration Wizard window, click Next.



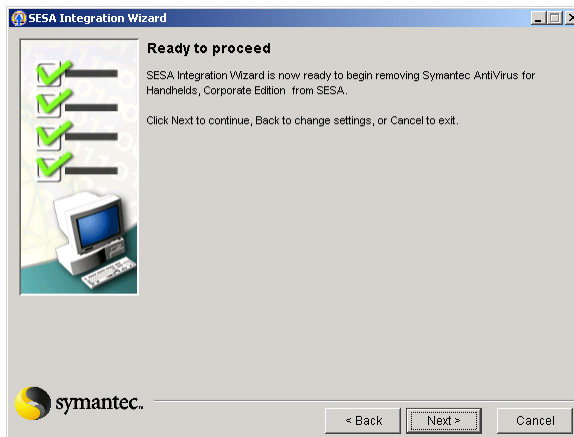
5 In the SESA Integration Requirements window, click **Next**.



The screenshot shows the 'SESA Integration Wizard' window. The title bar says 'SESA Integration Wizard'. The main area is titled 'SESA Domain Administrator Information'. It contains a text box with 'XXXXX.' and a diagram of a network. Below the diagram are four input fields: 'administrator' (SESA Domain Administrator Name), '*****' (SESA Domain Administrator Password), '255.255.255.255' (Host Name or IP Address of SESA Directory), and '636' (Secure Directory Port). A 'Status' section at the bottom says 'Connecting to the SESA Directory'. The Symantec logo is at the bottom left, and 'Back', 'Next >', and 'Cancel' buttons are at the bottom right.

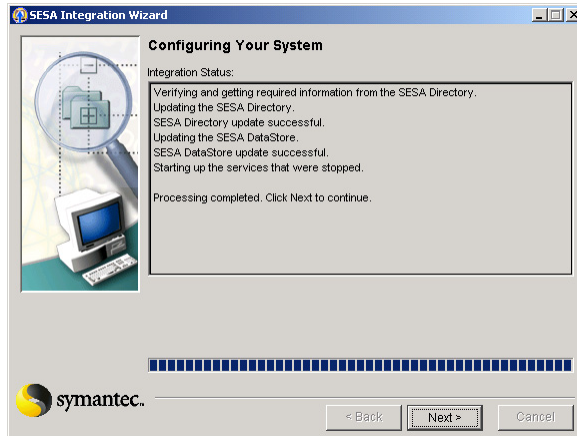
6 In the SESA Domain Administrator Information window, type the following, then click **Next**:

- The SESA Domain Administrator name
- The SESA Domain Administrator password
- The host name or IP address of the computer hosting the SESA Directory
- The Secure Directory port (by default, 636)

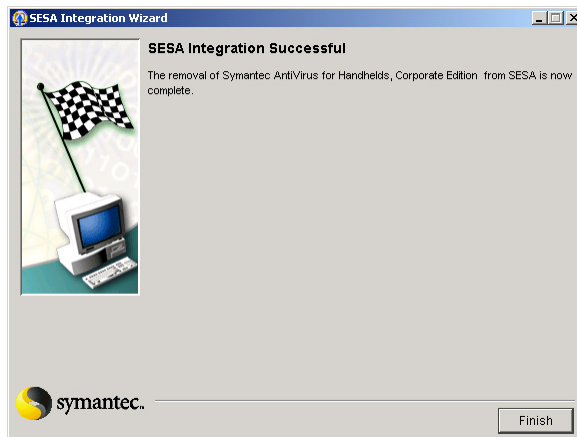


The screenshot shows the 'SESA Integration Wizard' window. The title bar says 'SESA Integration Wizard'. The main area is titled 'Ready to proceed'. It contains a list of four items, each with a green checkmark. Below the list is a diagram of a computer. The text says: 'SESA Integration Wizard is now ready to begin removing Symantec AntiVirus for Handhelds, Corporate Edition from SESA.' and 'Click Next to continue, Back to change settings, or Cancel to exit.' The Symantec logo is at the bottom left, and 'Back', 'Next >', and 'Cancel' buttons are at the bottom right.

- 7 In the Ready to proceed window, click **Next**.



- 8 When the uninstallation is complete, the Configuring Your System window displays the message “Processing completed. Click Next to continue.” Click **Next**.



- 9 In the SESA Integration Successful window, click **Finish**.

Scanning for and responding to viruses

This chapter includes the following topics:

- [About scanning for and responding to viruses](#)
- [Using Auto-Protect to automatically scan files](#)
- [Initiating an on-demand scan](#)
- [Configuring post-synchronization scans](#)
- [Scheduling repeating scans](#)
- [Configuring Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager](#)

About scanning for and responding to viruses

The Auto-Protect feature provides real-time scanning of files as they are accessed on the handheld device. In addition, you may perform scans on demand, after a synchronization, or according to a schedule.

Scan configuration options

Scan options are managed on the desktop and the handheld device. In a SESA environment, access to scan options on the desktop and handheld device may be disabled and all configuration may be managed from SESA.

Table 3-1 summarizes the scan configuration options and where they are configured.

Table 3-1 Scan configuration options

Platform	Options
Handheld device	<div>You can configure the following scan settings on the handheld device:</div> <ul style="list-style-type: none">■ Handheld Auto-Protect■ Post-synchronization scans■ Handheld device expansion card scans
Desktop	<div>You can configure the following scan settings on the desktop (when Symantec AntiVirus for Handhelds - Corporate Edition is managed by SESA, these settings are not configurable on the desktop):</div> <ul style="list-style-type: none">■ Handheld Auto-Protect■ Handheld device expansion card scans■ Locking post-synchronization scans■ Locking scan cancellation on the handheld device
SESA	<div>You can configure the following scan settings in the SESA Console:</div> <ul style="list-style-type: none">■ Enabling and locking the scanning of files after each synchronization■ Scanning files after the next synchronization■ Enabling and locking Auto-Protect on the handheld device■ Enabling and locking expansion card scans on the handheld device■ Disabling scan cancellation on the handheld device

Note: Settings on the handheld device that are not locked in the desktop override settings set in the desktop. In a SESA environment, all lockable settings are by default locked. You must explicitly unlock a setting in the SESA Console to make it configurable in Symantec AntiVirus for Handhelds - Corporate Edition.

Using Auto-Protect to automatically scan files

As files are accessed on the handheld device, Auto-Protect provides automatic, real-time virus scanning. When Symantec AntiVirus for Handhelds - Corporate Edition scans a suspicious file, it blocks access to the file and presents a dialog box that allows you to delete, allow, or (for Palm OS only) deny access to the file.

Using Auto-Protect on Palm OS handheld devices

[Table 3-2](#) summarizes what you can do when Auto-Protect finds a virus on your Palm OS handheld device.

Table 3-2 Auto-Protect options on Palm OS handheld devices

Option	Description
Delete	This action deletes the infected file and is the recommended action. After you tap Delete, a message appears telling you to reset your handheld device.
Deny Access	This action does not open the infected file and stops the current activity to prevent you from using an infected file.
Allow	This action continues the current activity. Select this action only if you are sure that a virus is not at work. You will receive an alert each time that you open the file. If you are not sure what to do, do not open the file.

Using Auto-Protect on Pocket PC handheld devices

[Table 3-3](#) summarizes what you can do when Auto-Protect finds a virus on a Pocket PC handheld device.

Table 3-3 Auto-Protect options on Pocket PC handheld devices

Option	Description
Delete	This action deletes the infected file and is the recommended action. After you tap Delete, a message appears telling you to reset your handheld device.
Allow	This action continues the current activity. Select this action only if you are sure that a virus is not at work. You will receive an alert each time that you open the file. If you are not sure what to do, do not open the file.

To use Auto-Protect to automatically scan files

- 1 On the desktop, in the main Symantec AntiVirus for Handhelds - Corporate Edition window, click **Configure**, then click **AntiVirus Configuration**.
- 2 Click **Handheld Auto-Protect**.

Initiating an on-demand scan

Initiate an on-demand scan if you think that the handheld device may contain a virus. This is particularly important if you have ever disabled Auto-Protect on the handheld device.

Note: If you initiate an on-demand scan with Handheld Expansion Card Scanning enabled, Symantec AntiVirus for Handhelds - Corporate Edition scans the expansion card for viruses.

To initiate an on-demand scan

- 1 On the handheld device, on the Symantec AntiVirus screen, tap **Scan**.
When the scan is complete, Symantec AntiVirus for Handhelds - Corporate Edition displays a list of any viruses found.
- 2 To remove a virus, tap an item in the list, then on the Symantec AntiVirus screen, click **Delete**.
See [“Scan configuration options”](#) on page 44.

Configuring post-synchronization scans

A one-time post-synchronization scan can be configured on the desktop. In addition, the desktop and handheld device can configure Symantec AntiVirus for Handhelds - Corporate Edition to scan after each synchronization.

Note: On Pocket PCs, post-synchronization scans only occur if the synchronization changes files on the handheld device. If there are no new or changed files to synchronize, no scan occurs.

See [“Scan configuration options”](#) on page 44.

Configure post-synchronization scans

Post-synchronization scans may be configured to occur after the next synchronization or after every synchronization.

To configure a scan after the next synchronization

- 1 On the desktop, in the Scans window, click **Scan After Synchronization**.
- 2 Click **Scan after next synchronization**.
Symantec AntiVirus for Handhelds - Corporate Edition automatically initiates a one-time scan after the next synchronization.

To configure a scan after each synchronization using the handheld device

- 1 On the Symantec AntiVirus screen, tap **Tools > Preferences**.
- 2 Tap **Scan all after synchronization**.

To configure a scan after each synchronization using the desktop

- 1 On the desktop, in the Scans window, click **Scan After Synchronization**.
- 2 Click **Always scan after synchronization**.

Scheduling repeating scans

Scheduled scans may be configured from the desktop.

Schedule repeating scans

A scheduled scan can repeat every day, every week, every month, or once at a specific date and time.

To schedule a scan that repeats every day, every week, or every month

- 1 On the desktop, in the Scans window, click **Scheduled Scan**.
- 2 Check **Enable scan**.
- 3 Select a daily, weekly, or monthly frequency.
- 4 Select the schedule for the scan.
- 5 Synchronize the handheld device.

To configure a one-time scan on a specific date

- 1 On the desktop, in the Scans window, click **Scheduled Scan**.
- 2 Check **Enable scan**.
- 3 Click **Once**.
- 4 Specify the year, month, day, and time for the scan.
- 5 Synchronize the handheld device.

Configuring Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager

In SESA environments, Symantec AntiVirus for Handhelds - Corporate Edition can be configured and controlled in the SESA Console. Configurations that are pushed from SESA override settings that are configured on the handheld device or desktop. By default, all lockable settings are disabled until you roll out a configuration that enables them. To disable or enable local access to configuration settings, use the lock options in the SESA Console.

See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager”](#) on page 28.

Modifying general configuration settings in SESA

The General tab contains the following information about the configuration:

- **Name:** The name of the configuration. This is an editable field.
- **Description:** A description of the configuration. This is an editable field.
- **Last modified on:** The last date on which the configuration was modified.

To modify the configuration name and description

- 1 In the main SESA Console window, on the Configurations tab, double-click the **Symantec AntiVirus for Handhelds, Corporate Edition** folder.
- 2 Double-click the configuration that you want to use.
- 3 On the General tab, in the right pane, modify the configuration name and description as necessary.
- 4 Click **Apply**.
See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager”](#) on page 28.

Configuring post-synchronization scans in SESA

The SESA Console may be used to configure Symantec AntiVirus for Handhelds - Corporate Edition to initiate a scan after synchronization.

A post-synchronization scan may be set to occur after the next synchronization or after every synchronization.

To configure a post-synchronization scan after the next synchronization or after every synchronization

- 1 In the main SESA Console window, on the Configurations tab, double-click the **Symantec AntiVirus for Handhelds, Corporate Edition** folder.
- 2 Double-click the configuration that you want to use.
- 3 On the Scan After Sync tab, in the right pane, do one of the following:
 - To scan after the next synchronization, in the Value column for the Scan after next synchronization property, click **True**.
 - To scan after every synchronization, in the Value column for the Always scan after synchronization property, click **True**.
- 4 Click **Apply**.
- 5 In the left pane, right-click the configuration, then click **Distribute**.
- 6 Click **Yes** to distribute the configuration settings to the computers that are defined in the configuration properties for that configuration setting.
See [“Configuring post-synchronization scans”](#) on page 47.

Configuring scheduled scans in SESA

Scheduled scans may be enabled and configured in the SESA Console.

Note: The SESA Console supports one scan schedule per named configuration. If you want to set up multiple scan schedules, you must create additional configurations.

To configure a scheduled scan in SESA

- 1 In the main SESA Console window, on the Configurations tab, double-click the **Symantec AntiVirus for Handhelds, Corporate Edition** folder.
- 2 Double-click the configuration that you want to use.
- 3 On the Scheduled Scan tab, in the right pane, specify the scanning schedule that you want to use.
- 4 Click **Apply**.
- 5 In the left pane, right-click the configuration, then click **Distribute**.
- 6 Click **Yes** to distribute the configuration settings to the computers that are defined in the configuration properties for that configuration setting.
See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager”](#) on page 28.
See [“Scheduling repeating scans”](#) on page 47.

Configuring and locking AntiVirus options in SESA

To disable or enable local access to configuration settings, use the lock options that are in the SESA Console. Configurations rolled out from SESA override settings that are configured on the handheld device or desktop. By default, all lockable settings are disabled until you roll out a configuration that enables them.

To configure and lock AntiVirus options in SESA

- 1 In the main SESA Console window, on the Configurations tab, double-click the **Symantec AntiVirus for Handhelds, Corporate Edition** folder.
- 2 Double-click the configuration that you want to use.
- 3 On the AntiVirus tab, in the right pane, specify the AntiVirus scanning values that you want to use.
- 4 Specify the locked state for the AntiVirus settings.

- 5 In the left pane, right-click the configuration, then click **Distribute**.
- 6 Click **Yes** to distribute the configuration settings to the computers that are defined in the configuration properties for that configuration setting.

Configuring LiveUpdate Wireless options in SESA

LiveUpdate Wireless allows handheld devices with wireless Internet connectivity to update their virus definitions files over the Internet. Configuring handheld devices to use LiveUpdate Wireless allows users to keep their virus protection up-to-date while using a handheld device away from the desktop for an extended period of time.

To configure LiveUpdate Wireless options

- 1 In the main SESA Console window, on the Configurations tab, double-click the **Symantec AntiVirus for Handhelds, Corporate Edition** folder.
- 2 Double-click the configuration that you want to use.
- 3 On the LiveUpdate Wireless tab, in the right pane, specify the LiveUpdate Wireless settings that you want to use.
- 4 Click **Apply**.
- 5 In the left pane, right-click the configuration, then click **Distribute**.
- 6 Click **Yes** to distribute the configuration settings to the computers defined in the configuration properties for that configuration setting.
 See [“Installing Symantec AntiVirus for Handhelds - Corporate Edition with Event and Configuration Manager”](#) on page 28.
 See [“Using LiveUpdate to update Symantec AntiVirus for Handhelds - Corporate Edition”](#) on page 56.
 See [“To configure LiveUpdate Wireless on the desktop”](#) on page 57.

Setting an administrator message in SESA

Administrator messages appear in the desktop’s Administration Configuration window and in the handheld device’s About AntiVirus dialog box. You can push a custom message using the SESA Console.

To set an administrator message in SESA

- 1 In the main SESA Console window, on the Configurations tab, double-click the **Symantec AntiVirus for Handhelds, Corporate Edition** folder.
- 2 Double-click the configuration that you want to use.
- 3 On the Administrator tab, in the right pane, in the value column next to the Admin Message property, type an administrator's message.
- 4 Click **Apply**.
- 5 In the left pane, right-click the configuration, then click **Distribute**.
- 6 Click **Yes** to distribute the configuration settings to the computers defined in the configuration properties for that configuration setting.

Updating Symantec AntiVirus for Handhelds - Corporate Edition

- [About updating Symantec AntiVirus for Handhelds - Corporate Edition](#)
- [Using LiveUpdate to update Symantec AntiVirus for Handhelds - Corporate Edition](#)

About updating Symantec AntiVirus for Handhelds - Corporate Edition

Symantec AntiVirus for Handhelds - Corporate Edition supports the following update methods:

- Virus definitions files updates: Symantec products use virus definitions files to identify viruses. Symantec Security Response researches and responds to new virus threats and provides customers with virus definitions files updates as new viruses emerge.
- Software updates: Symantec occasionally provides software patches that fix software issues with Symantec AntiVirus for Handhelds - Corporate Edition.

Symantec AntiVirus for Handhelds - Corporate Edition updates may be accessed through several methods. [Table 4-1](#) lists and describes each update method.

Table 4-1 Update methods

Method	Description	When to use it
LiveUpdate	A scheduled or manual pull operation that starts when a client or server on which LiveUpdate is being used requests new definitions. LiveUpdate may be configured on each desktop to request the update from a designated internal LiveUpdate server or directly from the Symantec LiveUpdate server.	Use LiveUpdate when you want desktops to automatically update their virus definitions files or users to manually update their virus definitions files.
LiveUpdate Wireless	A manually initiated pull operation that starts when a user with a handheld device on which LiveUpdate Wireless is being used requests new virus definitions. LiveUpdate requests the update directly from the Symantec LiveUpdate server.	Use LiveUpdate Wireless when you have handheld devices that have wireless Internet connectivity, and that infrequently or never synchronize with a desktop.

Table 4-1 Update methods

Method	Description	When to use it
Virus Definition Transport Method	A push operation that starts when new virus definitions are received via the Symantec FTP site or LiveUpdate server by a primary server on your network. The primary server passes a virus definitions package to all of the secondary servers in the server group. Secondary servers extract the virus definitions and place them in the appropriate directory. Clients receive the package from their parent servers. Clients extract the virus definitions and place them in the appropriate directory.	Use the Virus Definition Transport Method when you use Symantec Client Security and want to control virus definitions file updates from the Symantec System Center. In addition, use this method during a virus outbreak to push the latest virus definitions files to the desktops on your network immediately. For more information, see the <i>Symantec Client Security Administrator's Guide</i> .
Intelligent Updater	A self-extracting executable file that contains virus definitions files.	Use Intelligent Updater when you need to distribute virus definitions files updates to users who do not have active network connections. For more information, see the <i>Symantec Client Security Administrator's Guide</i> .

Using LiveUpdate to update Symantec AntiVirus for Handhelds - Corporate Edition

By default, Symantec AntiVirus for Handhelds - Corporate Edition is configured to do the following:

- Use LiveUpdate on the desktop to automatically or manually update both virus definitions files and the Symantec AntiVirus for Handhelds - Corporate Edition software. LiveUpdate can automatically check for an Internet connection in five-minute intervals. When LiveUpdate is able to connect to the Internet, it downloads the latest virus definitions update files and installs them on the desktop. Following the initial download, LiveUpdate checks for updates at four-hour intervals. LiveUpdate may be configured from the desktop.
- Perform an Express LiveUpdate session, in which there is no user interaction. This configuration setting may be modified in the desktop and in the SESA Console in SESA environments.
- Allow handheld devices to initiate a LiveUpdate Wireless session. This configuration setting may be configured in the desktop and configured and locked in the SESA Console. Users may view but not modify a locked setting.

Note: If the handheld device is configured to update using LiveUpdate Wireless but does not have an active Internet connection, an error dialog box appears when users attempt to initiate a LiveUpdate Wireless session.

Configure LiveUpdate options

To use LiveUpdate Wireless, the handheld device must have wireless Internet connectivity, and, if your network uses proxies, the appropriate proxy settings in order to connect to the Internet via a proxy server.

To configure LiveUpdate on the desktop

- 1 In the main Symantec AntiVirus for Handhelds - Corporate Edition window, click **File > Configure Desktop LiveUpdate**.
- 2 In the Configure Desktop LiveUpdate window, check **Enable Automatic LiveUpdate** to enable Automatic LiveUpdate.

- 3 Select one of the following:
 - Apply updates without interrupting me: Enables Express LiveUpdate. The desktop will automatically initiate a LiveUpdate session.
 - Notify me when updates are available: Offers the option of beginning a LiveUpdate session when virus definitions files updates are available.
- 4 Click **Apply**.

To configure LiveUpdate Wireless on the desktop

- 1 In the main Symantec AntiVirus for Handhelds - Corporate Edition window, double-click **Configure**.
- 2 Click **LiveUpdate Wireless Configuration**.
- 3 Check **Use LiveUpdate Wireless Server**.

To configure and lock LiveUpdate Wireless in SESA

- 1 In the main SESA Console window, on the Configurations tab, double-click the **Symantec AntiVirus for Handhelds, Corporate Edition** folder.
- 2 Double-click the configuration that you want to use.
- 3 On the LiveUpdate Wireless tab, in the right pane, specify the LiveUpdate wireless settings that you want to use.
- 4 Click **Apply**.
- 5 In the left pane, right-click the configuration, then click **Distribute**.
- 6 Click **Yes** to distribute the configuration settings to the computers defined in the configuration properties for that configuration setting.

To set proxy server settings for LiveUpdate Wireless using the desktop

- 1 In the main Symantec AntiVirus for Handhelds - Corporate Edition window, double-click **Configure**, then click **LiveUpdate Wireless Configuration**.
- 2 Click **Use HTTP Proxy**.
- 3 Type the proxy settings for your network.

To set proxy server settings for LiveUpdate Wireless using the handheld device

- 1 On the Symantec AntiVirus screen, tap **Tools > LiveUpdate**.
- 2 On the LiveUpdate screen, tap **Tools > Preferences**.
- 3 Tap **Use HTTP Proxy**.
- 4 Type the proxy settings for your network.
- 5 Click **OK**.

To set and lock proxy server settings for LiveUpdate Wireless server settings in SESA

- 1 In the main SESA Console window, on the Configurations tab, double-click the **Symantec AntiVirus for Handhelds, Corporate Edition** folder.
- 2 Double-click the configuration that you want to use.
- 3 On the LiveUpdate Wireless tab, in the right pane, specify the appropriate proxy server settings.
- 4 Click **Apply**.
- 5 In the left pane, right-click the configuration, then click **Distribute**.
- 6 Click **Yes** to distribute the configuration settings to the computers defined in the configuration properties for that configuration setting.

Viewing and configuring histories, events, and alerts with Symantec AntiVirus for Handhelds - Corporate Edition

This chapter includes the following topics:

- [About histories, events, and alerts](#)
- [Working with histories on the handheld device](#)
- [Working with histories on the desktop](#)
- [Viewing and configuring events and alerts in SESA](#)

About histories, events, and alerts

The handheld device maintains a local history of any antivirus activity. The data may be viewed directly on the handheld device. When the handheld device is synchronized with a desktop, its history data is uploaded to the desktop, where it may be viewed on the desktop. In SESA environments, the SESA Agent forwards the data to the SESA Manager, where it may be viewed in the SESA Console. In addition, the SESA Console can be configured to trigger alerts based on the events that it receives.

Note: Given the screen space limitations of handheld devices, only a subset of a handheld device’s history data is viewable on the handheld device. The full set of history data is viewable on the desktop.

[Table 5-1](#) lists and describes the history data that is recorded by the handheld device.

Table 5-1 Histories recorded by the handheld device

History	Description
Partial scans	A partial scan entry is added when a user cancels a scan, or only scans part of the handheld device (for example, only the handheld device’s main memory, and not its expansion card).
Full scans	A full scan entry is added when the entire handheld device, including any expansion cards, is scanned.
Found viruses	A found virus entry is added whenever Symantec AntiVirus for Handhelds - Corporate Edition identifies a file that is infected with a virus.
Deleted files	A log entry is added when a user uses Symantec AntiVirus for Handhelds - Corporate Edition to delete an infected file.

When the handheld device is synchronized with a desktop, its history data is uploaded to the desktop, where it may be viewed. In a SESA environment, the SESA Agent forwards the data to SESA, where its is viewable in the SESA Console.

See [“How histories are logged”](#) on page 13.

Working with histories on the handheld device

You can use the Activity Log on the handheld device to view the antivirus activities on the handheld device.

Work with entries in the Activity Log

The Activity Log displays antivirus activity on the handheld device and also lets you delete activities from the log.

To work with entries in the Activity Log on Pocket PC handheld devices

- 1 On the handheld device, on the Symantec AntiVirus screen, tap **Tools > Activity Log**.
- 2 If you want to view details or delete an entry, tap the entry.
- 3 On the Log Detail screen, tap **Delete** to delete the entry.
- 4 In the confirmation dialog box, tap **Yes**.

To work with entries in the Activity Log on Palm OS handheld devices

- 1 On the handheld device, on the Symantec AntiVirus screen, tap **Menu > Activity Log**.
- 2 Do one of the following:
 - To delete an entry, tap **Delete**.
 - To clear the Activity Log of all entries, tap **Clear All**.See [“Working with histories on the desktop”](#) on page 61.

Working with histories on the desktop



The desktop component of Symantec AntiVirus for Handhelds - Corporate Edition provides three categories of activities:

- Virus
- Scan
- Event

In addition, the desktop can purge all log data.




The virus history displays information about viruses identified on the handheld device. [Table 5-2](#) describes the values displayed for the virus history.

Table 5-2 Virus History

Data displayed	
The virus history displays the following data:	
■	File status, displayed as one of the following icons: Deleted:  Allowed: 
■	Date the virus was discovered
■	Device type
■	Operating system
■	Operating system version
■	Profile/Partnership name
■	Name of the virus
■	Virus number
■	The Virus Definition version that was used to discover the virus
■	Type of infected item
■	Path of infected files
■	Path to the file that is inside of a compressed file
■	Status of the item that is inside of a container file
■	File size
■	The ID of the scan in which the virus was discovered









The virus history displays information about scans performed on the handheld device. [Table 5-3](#) describes the values displayed for the scan history.

Table 5-3 Scan History

Data displayed
<p>The scan history displays the following data:</p> <ul style="list-style-type: none">■ Action type, displayed as one of the following icons: Scan started:  Scan ended:  Scan cancelled: ■ Scan date■ Device type■ Device operating system■ Operating system version■ Profile/Partnership name■ Scan description■ Scan ID■ Scan type: Manual or scheduled

The virus history displays information about events on the handheld device. [Table 5-4](#) describes the values displayed for the event log.

Table 5-4 Event Log

Data displayed
<p>The event history displays the following data:</p> <ul style="list-style-type: none">■ Event type, displayed as one of the following icons: Virus definitions files update:  Auto-Protect enabled:  Auto Protect disabled:  Application update:  Synchronization start:  Synchronization end:  Profile name changed:  ■ Event date■ Device type■ Device operating system■ Operating system version■ Profile/Partnership name■ Virus Definition Update: The version number of the definition file■ Configuration Change: The source of the configuration change (user or administrator)■ Application Update: The application revision number■ Sync: The unique synchronization ID assigned by Symantec AntiVirus for Handhelds - Corporate Edition

Work with histories on the desktop

The desktop can display all logged histories, the histories for the day, the week, the month, or histories filtered by a specified date range. In addition, you can also delete history data from the desktop.

To display history data for today, the past seven days, the current month, or all items

- 1 On the desktop, in the main Symantec AntiVirus for Handhelds - Corporate Edition window, click **Histories**.
- 2 In the Symantec AntiVirus for Handhelds - Corporate Edition window, in the right pane, select the type of history that you want to view.
- 3 Click the list box, then select one of the following:
 - Today
 - Past 7 Days
 - This Month
 - All Items
- 4 Double-click an event to view its details.

To display history data for a selected date range

- 1 On the desktop, in the main Symantec AntiVirus for Handhelds - Corporate Edition window, click **Histories**.
- 2 In the Symantec AntiVirus for Handhelds - Corporate Edition window, in the right pane, select the type of history that you want to view.
- 3 Click the list box, then click **Selected Range**.
- 4 In the Date Range Filter dialog box, type a Start Date and an End Date.
- 5 Click **OK**.
- 6 Double-click an event to view its details.

To purge log data using the desktop

- 1 On the desktop, in the main Symantec AntiVirus for Handhelds - Corporate Edition window, click **Histories > Purge Log History**.
- 2 Click **Yes**.
See [“Working with histories on the handheld device”](#) on page 61.

Viewing and configuring events and alerts in SESA

In a SESA environment, the SESA Agent queues events on the desktop and sends them to the SESA Manager. The Manager logs the events in the SESA DataStore, where they may be viewed in the SESA Console.

Alerts consolidate event data and provide notification services. You can create an alert based on a specific event or multiple occurrences of an event over a period of time.

For more information on configuring alerts, see the SESA documentation.

To view Symantec AntiVirus for Handhelds - Corporate Edition event reports in SESA

- 1 In the SESA Console, on the Events tab, double-click **AntiVirus Event Family**.
- 2 Under AntiVirus Event Family, double-click **AntiVirus Handhelds**.
- 3 Select one of the following reports:
 - All Virus Incidents: Provides a tabular view of virus incidents
 - All Scans: Provides a tabular view of scanning activity
 - Action Summary: Provides a pie chart report of antivirus activities
 - Virus Locations: Provides a bar chart report of the location of viruses identified by Symantec AntiVirus for Handhelds - Corporate Edition

See [“Working with histories on the handheld device”](#) on page 61.

See [“Working with histories on the desktop”](#) on page 61.

Index

A

AntiVirus options
 configuring with SESA 50

Auto-Protect
 about 44, 45
 enabling 46
 Palm OS handheld devices 45
 Pocket PC handheld devices 46

C

configuration
 locking 45

E

EICAR 38

H

histories
 about 13, 60
 Activity Log 16, 61
 deleting entries from Activity Log 61
 on desktop 61, 65
 purging on desktop 65
 types of histories 60

I

installation
 hardware requirements 21
 installing the SESA Agent remotely 32
 remote 27
 SESA 28
 SESA Integration Package 32
 silent 17, 27
 silent installation switches 27
 software requirements 20
 synchronizing with handheld devices 26
 testing 37

uninstalling 38
 consumer version 21
 the SESA Integration Package 39
 using a remote administration tool 17

L

license
 distributing 23
 obtaining 22
 serial number 11, 21

LiveUpdate
 configuring with SESA 51
 desktop 13
 Express 56
 software updates 12
 virus definitions files updates 12
 Wireless 13, 15

S

scans
 after next synchronization 47
 Auto-Protect 11, 12, 15, 44, 45
 configuring from SESA 44
 configuring with Event and Configuration Manager 48
 expansion card 44
 on-demand 12, 46
 post-synchronization 12, 47, 49
 configuration with SESA 49
 on Pocket PC 47
 scheduled 12, 47
 scheduled configuration with SESA 50

SESA 16
 administrator message 51
 Agent 14, 66
 alerts 13, 66
 DataStore 66
 events 13, 66
 Integration Package 14

- Manager 66
 - IP address 31
 - port number 31
- reports 66
- Symantec AntiVirus Corporate Edition 15

U

- updates
 - configuring LiveUpdate 56
 - configuring LiveUpdate Wireless 57
 - Intelligent Updater 55
 - LiveUpdate Wireless 54
 - LiveUpdate, on desktop 56
 - proxy server settings 57
 - software 54
 - Virus Definition Transport Method 55
 - virus definitions files 54

V

- viruses
 - allowing 45, 46
 - deleting 45, 46
 - denying access 45
 - logging virus events 12